To protect user privacy online, governments need to reconsider their use of opt-in policies

February 18 2024, by Raymond A. Patterson, Hooman Hidaji, Niam Yaraghi, Ram Gopal and Sule Nur Kutlu

Credit: Pixabay/CC0 Public Domain

Internet users—almost all of us—are growing used to seeing requests for consent to gather our information: "Do you accept cookies from this website?" Most of us just click "yes" and continue browsing, rather than

bothering with convoluted settings and choices we don't quite understand.

Consumers are not too happy with these requests and some even look for ways to avoid them. These pop-ups are in response to recent data protection and privacy regulations, such as the European Union's General Data Protection Regulation and California's Consumer Privacy Act.

Other jurisdictions are looking to implement their own sets of regulations, including Canada, which is in the process of reviewing and modernizing the Privacy Act.

Such regulations are intended to limit the collection of data on users and users' exposure to third parties, but our analysis suggests these regulations may not be as effective as intended. Our research has found they actually increase the use of third parties that access user data and decrease competition to the detriment of consumers.

Commodification of user data

Almost every website—both for-profit and not-for-profit—commodifies user data. Within the first three seconds of opening a web page, over 80 third parties on average have accessed your information.

The usage of user data by third parties can be helpful, as it is an easy way for companies to earn money and it can easily connect consumers to any resources they are looking for.

But third parties can also pose serious privacy threats to consumers, which is why privacy legislation is needed. Privacy threats can result in financial harm to users and society at large. For example, discrimination can be based on any detectable characteristic, including psychographic

profiles, age, race, gender, religious affiliation and others.

Society at large can be harmed by coordinated attempts to manipulate voters, as was the case with the Cambridge Analytica scandal.

Moreover, the strategic reaction of the websites to regulation is often overlooked. There is a cat and mouse game in reaction to regulation—they are not a matter of simple compliance.

If a regulation says a website has to do X, then a website will react to that limitation and do Y while also doing X. Strategic reactions are not necessarily to avoid compliance, but rather to maximize profit in response to new regulatory requirements.

The impact of privacy policies

Our research group, consisting of scholars including Ram Gopal from the University of Warwick, Niam Yaraghi from the University of Miami, and Hooman Hidaji, Sule Kutlu and Ray Patterson from the University of Calgary, have spent years studying website privacy and revenue management.

Previously, we analyzed the privacy implications of website monetization strategies and the prediction of website trustworthiness by observing their third-party usage. Recently, our focus has shifted to studying the impact of data regulation on consumers and websites to understand the impact of new privacy policies.

In our recent study, published in *Information Systems Research*, we studied the effects of government intervention to protect consumer privacy online. We collected third-party utilization of the most popular 100,000 websites globally when California's Consumer Privacy Act (CCPA) went into effect.

Comparing jurisdictions with and without opt-in policies, we found that the implementation of opt-in policies had an unintended effect on the use of third parties: there was a significant increase in the number of third parties when accessing websites from California after CCPA went into effect.

We also found that, in markets where some users had relatively low privacy concerns, opt-in laws had the unintended consequence of increasing the number of third parties, thereby increasing the privacy exposure of users.

Learning from past mistakes

Our findings have important implications for policymakers involved in data protection and privacy regulation. In Canada, where privacy regulation is not yet finalized, there is an opportunity to learn from the mistakes of other regulators.

As our research has found, opt-in policies are counterproductive in addressing third-party data-sharing concerns and can harm competition. Instead, we recommend using a mix of policies that are used in a more precise manner, rather than the currently preferred one-size-fits-all policies.

More precisely targeted mechanisms, such as limited consent requirements and subsidizing websites in particular sectors or industries, motivate competing websites to improve their third-party data sharing. Website subsidization acts like a precise tool, allowing policymakers to impact specific target markets.

Opt-in policies, on the other hand, are more comparable to a sledgehammer that uniformly affects all market segments. Rather than globally implementing legislation, we advocate for a combination of

policies and local subsidies that are better suited to an industry's specific needs.

Provided by The Conversation